

Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) EP 0 697 662 A1

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:  
21.02.1996 Bulletin 1996/08

(51) Int. Cl.<sup>6</sup>: G06F 12/14, G06F 1/00

(21) Application number: 94112649.2

(22) Date of filing: 15.08.1994

(84) Designated Contracting States:  
DE FR GB

(71) Applicant: International Business Machines  
Corporation  
Armonk, N.Y. 10504 (US)

(72) Inventors:  
• Deinhart, Klaus  
D-71272 Renningen (DE)

• Gligor, Virgil D., Dr.  
Chevy Chase, MD 20815 (US)  
• Lingenfelder, Christoph, Dr.  
D-69190 Walldorf (DE)  
• Lorenz, Sven, Dr.  
D-70180 Stuttgart (DE)

(74) Representative: Schäfer, Wolfgang, Dipl.-Ing.  
D-70548 Stuttgart (DE)

### (54) Method and system for advanced role-based access control in distributed and centralized computer systems

(57) A method and system for registration, authorization, and control of access rights in a computer system are disclosed in the present invention. The inventive method for controlling access rights of subjects (1) on objects (4) in a computer system uses parameterized role types (2) that can be instantiated into role instances (4) equivalent to roles or groups as known from the prior art. The required parameters are provided by the subject (1) of the computer system, e.g. by a person (5), a job position (6) or an organization unit (7). Furthermore, the inventive method provides relative resource sets (8) which are instantiated into concrete resource sets (9)

and individual resources (10) by using the same parameter values as for instantiating the role types.

The inventive system for authorization and control of access rights as disclosed in the present invention comprises capability lists (30) providing the access rights of the subjects (1) on the objects (4) of a computer system on a per-subject basis. Furthermore, the inventive system comprises means for deriving (32) access control lists (31) from capability lists (30), wherein said access rights of the subjects (1) on the respective objects (4) are provided.

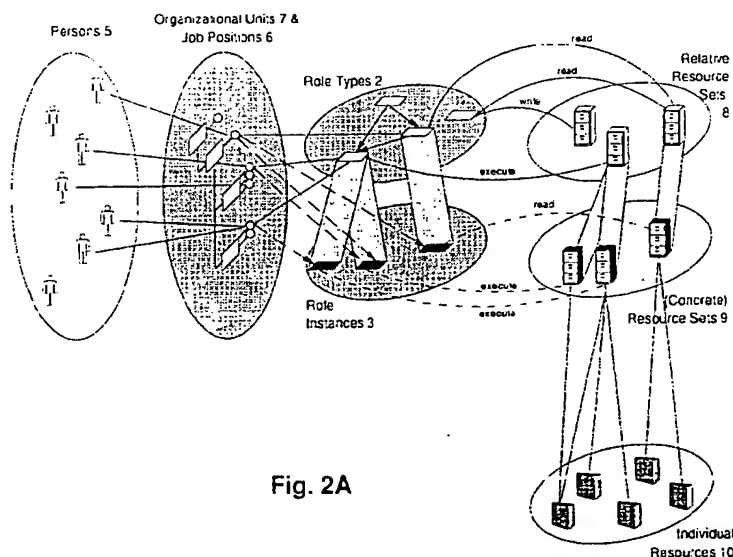


Fig. 2A

EP 0 697 662 A1

## Description

### Technical Field

The present invention relates to the technical field of role-based access control methods and security systems in distributed and centralized computer systems. More specifically, the invention relates to a method for controlling access rights of subjects on objects in a computer system by controlling said access rights dependent on a membership of a subject to a role. Furthermore, the invention relates to a system for registration, authorization, and control of access rights of subjects on objects in a computer system, wherein the system comprises users, groups, and access control lists at each object providing the access rights on the respective object.

### Background Art

In a computer system the accesses of users to data have to be controlled for security needs of the enterprise or organization using this computer system. The control of these accesses is performed by using access rights defining whether and how a user may access data in the computer system. This access control is performed by a security system which is integrated in or added to the operating system of the computer system. This security system performs a specific method for controlling access rights.

In most of the installed computer systems access rights are granted or revoked explicitly for individual users or group of users on respective data or, more generally, on respective objects by a system administrator. All access rights of all users on this object are forming an access control list (ACL) associated to this object. When an access request occurs during operation time of the computer system from a user or, more generally, from a subject to this object, then the security system looks at the access control list of the respective object and decides whether the subject may access this object in the requested manner. These broadly installed security systems allow a so-called "per-object-review" of access rights, that is, to determine the kind of access rights of all subjects of a computer system to a respective object.

Since it is very inconvenient for a system administrator to provide each user with individual access rights, and for achieving a higher grade of data security and integrity in a computer system, a Role-Based Access Control (RBAC) method has been developed. Therein, a role is mainly a definition of a job at the lowest level of granularity used in this enterprise or organization. In this role-based access control system the system administrator only has to grant or revoke access rights to a role and has to group different subjects under this role.

In F.H. Lochovsky: "Role-Based security in Data Base Management systems" which is incorporated in C.E. Landwehr (editor): "Database Security: Status and Prospects", Elsevier Science Publishers B.V., 1988, pp.

209 - 222, the use of roles and objects in specifying a security mechanism for data base management systems is discussed. Using the idea that a user can play certain roles, authorization was specified using these roles.

In R.W. Baldwin: "Naming and Grouping Privileges to Simplify Security Management in Large Data Bases", Proceedings of IEEE Symposium on Security and Privacy, Oakland, 1990, pp. 116 - 132, authorization and controlling access rights in large security systems in the field of data base objects are described.

In D. Ferraiolo et al: "Role-Based Access Controls", Proceedings of the 5th National Computer Security Conference, Oct. 1992, pp. 554 - 563, which can be regarded as the closest prior art to the present invention, the role-based access control method is described in detail. Access control decisions are often based on the roles individual users take on as part of an organization. A role specifies a set of transactions that a user or set of users can perform within the context of an organization. Role-based access control provides a means of naming and describing relationships between individuals and access rights, providing a method of meeting the secure processing needs of many commercial and civilian government organizations.

Concerning the method of controlling access rights in a computer system as known from the existing role-based access control methods it is disadvantageous that a large number of similar but not identical job positions in an organization requires a large number of roles. This large number of roles causes a high storage requirement for the security system within the computer system. Furthermore it is disadvantageous, that the large number of roles causes high computing requirements for the security system. Both aspects lead to high costs for the operation of the security system. Furthermore, it is disadvantageous that the large number of roles makes it very difficult to manage the security system. The system administrator has to create a new role when a person remains in his job position but changes his location or project. This will cause higher costs or even less system security. Furthermore, since a role includes the union of all accesses and objects which users of that role have in different organization units of the enterprise. This means that the role will not necessarily contain the least privileges necessary for the functions of that role, i.e., a violation of the "Least Privilege Principle". However, if one attempts to mitigate the lack of access granularity with defining different roles based on access and object contexts, which may be possible in some designs, an administrative mechanism becomes necessary to relate these roles so that their consistent administration, e.g., update, becomes possible. Such a mechanism is not available today.

Concerning the access control system it is disadvantageous, that the existing role-based access control systems do not use the existing security mechanisms of the installed computer systems based on the existence of access control lists. Therefore, new security mechanisms or even a new security systems have to be imple-

mented on the existing computer system. This causes additional hardware and software development with related high costs. This is even more disadvantageous in distributed or large centralized computer systems. Existing standard access control mechanisms for distributed systems as described in "Introduction to OSF DCE", Open Software Foundation (OSF), 1991, allow scalability to very large distributed systems. To date no role-based access control method scalable to large distributed systems exists.

#### Objects of the Invention

It is an object of the invention to provide a method for controlling access rights that is scalable to very large distributed computer systems and requires less storage and computing performance for the security system. Furthermore, it is an object of the invention to provide a role-based method for controlling access rights that does not necessarily violate the "Least Privilege Principle" but at the same time is more flexible and more convenient for the system administration.

Concerning the system for authorization and control of access rights it is an object of the invention to provide a system that can use the security system of installed computer systems based on access control lists.

#### Summary of the Invention

The objects of the invention are fulfilled by the features of independent claims 1 and 13. Further arrangements of the invention are disclosed in the according dependent claims.

A method and system for registration, authorization, and control of access rights in a computer system are disclosed in the present invention. The inventive method for controlling access rights of subjects on objects in a computer system uses parameterized role types that can be instantiated into role instances equivalent to roles as known from the prior art. The required parameters are provided by the subject of the computer system. The computer system may derive the parameters from the job position of a subject or its membership in an organization unit. Furthermore, the inventive method provides relative resource sets which are instantiated into concrete resource sets and individual resources by using the same parameter values as for instantiating of role types.

The inventive system for authorization and control of access rights as disclosed in the present invention comprises capability lists providing the access rights of the subjects on the objects of a computer system on a per-subject basis. Furthermore, the inventive system comprises means for deriving access control lists from the capability lists, wherein the system provides said access rights of the subjects on the respective objects on a per-object basis. Within the inventive method, subjects are all possible types of holders of access rights within said computer system as for example persons, job positions, role instances, users, and transactions. Fur-

thermore, objects are all possible types of resources on which access rights can be defined within the computer system as for example files, disks, displays, printers, scanners, and transactions.

The invention as described in independent claim 1 eliminates the disadvantages previously described for the prior art. A method for controlling access rights providing role types that can be instantiated into role instances offers the possibility to design a security system for a computer system with very high flexibility. Since only a small number of role types has to be defined it is advantageous that less computing resources have to be provided for the security system within the computer system. Furthermore, it is advantageous that less administration activities caused by the definition of only a small number of role types requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security. Furthermore, it is advantageous that by providing the appropriate parameter values the role instances of a role type can be restricted in such a way that the "Least Privilege Principle" is satisfied. Furthermore, it is advantageous that the automated generation of role instances by instantiating role types offers higher security of the computer system and higher integrity of the data within the computer system.

A role type combines a set of functional tasks with a common generic set of competences. A role type can be viewed as a template for defining the types of access rights, objects, and transactions necessary to carry out a set of functional tasks.

A role instance, on the other hand, defines the set of concrete and specific competences bound to a role type in a specific organization unit of the enterprise. An organization unit may be division, a department, a program, a project, a work-flow process or a combination thereof.

In one embodiment of the invention as described in claim 2 the role type is parameterized and the role instance is generated by using at least one parameter value. The use of a parameterized role type allows more flexibility of the security system and less administration activities. Furthermore, it is advantageous that the use of parameterized role types requires less computing resources for the security system.

In a further embodiment of the invention as described in claim 3 the objects of the computer systems are forming groups of concrete resource sets. Forming of such concrete resource sets is advantageous since it allows to address functional groups of resources or objects with less computing efforts of the security system and less administrative overhead.

In a further embodiment of the invention as described in claim 4 the inventive method allows the automated derivation of the concrete resource sets from parameterized relative resource sets. This offers a higher flexibility of the security system with less administration efforts. Furthermore, it is advantageous that

less computing resources are required for the security system.

In a further embodiment of the invention as described in claim 5, the inventive method provides the parameter value for instantiating the parameterized role types or the parameterized relative resource sets by the subjects of the computer system. This is advantageous since the derivation of role instances from role types or the derivation of concrete resource sets from relative resource sets can be fully automated and requires no administration efforts. This restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment of the invention as described in claim 6 the parameter value is provided by the job position or by the organization unit. This is advantageous since it provides a very flexible security system that requires very little administration activity when a person as a user of the computer systems changes its job position or even the organization unit. This requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment of the invention as described in claim 7 the job position is combined with at least one role type. This is advantageous since it allows the deriving of role instances associated with this role type by providing all necessary parameters for instantiating a role type with this job position. This allows automated derivation of role instances with no administration activity and therefore requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further step of the invention as described in claim 8 the parameterized relative resource sets are associated with the role types. This is advantageous since it allows automated derivation of the concrete resource sets and objects by the same parameters as provided for the role types. This allows automated derivation of the concrete resource sets with no administration activities and therefore requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further step of the invention as described in claim 9 the inventive method performs a configuration step for deriving the role instances and the concrete resource sets and objects. This automated configuring step is performed with each administration action and provides at any time the actual and valid role instances and concrete resource sets and objects. This is advantageous since it guarantees the efficiency of the security system and guarantees the security and integrity of data within the computer system.

In a further embodiment of the invention as described in claim 10 the inventive method specifies capability list types associated with the role types and performs an automated configuring step for deriving capability lists associated with role instances. The capability lists are instantiated from the capability list types by

using the same parameters as for instantiating role types and these capability lists provide the access rights of the role instances on the objects within the computer system. The provision of capability lists within the security system of the computer system is advantageous, since it allows an automatic examination of the access rights of all subjects on all possibly objects within the computer system without any administration activities and therefore requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment of the invention as described in claim 11 the inventive method generates or modifies access control lists associated with the concrete resource sets and objects. This is advantageous since it supports the security systems as known from the prior art and as used within a large number of installed computer systems with all information required from these security systems. Therefore, the inventive method can be easily applied to the existing security systems without difficult modification or even expensive new implementation of the security system. In the case of scalable existing security systems for large distributed environments this method guarantees scalability of the role-based access control mechanism as well.

In a further embodiment of the invention as described in claim 12 the role types are organized hierarchically. This is advantageous since it allows the organization of role types by subsuming relations. Therefore, if a first role type subsumes a second role type then the set of access rights available to an instance of the first role type includes those available to a corresponding instance of the second role type. This allows a very easy control of access rights with only little administration efforts. Furthermore, it is advantageous that the hierarchical organization of role types requires less computing resources of the security system.

With the invention related to a computer system for authorization and control of access rights as described in independent claim 13, the disadvantages previously described for the prior art are eliminated. The registration, authorization, and control system presented in this application offers the advantage that access control lists at the object as well as capability lists at the subjects are provided. This allows a fast review of the access rights of a subject on all possible objects with only little computing resources for the security system. Furthermore, it allows a quick review of all access rights of all possible subjects on a specific object with only little computing resources for the security system. Furthermore, it is advantageous that a system comprising access control lists at the object as well as capability lists at the subject may be applied to all computer systems installed in the field without any change or new implementation in the operating system of the installed computer systems. Furthermore, the simultaneous existence of access control lists and capability lists offers high data security and integrity within the computer system. This is even more advantageous for large distributed computer systems.

In a further embodiment of the invention as described in claim 14 the inventive system comprises means that derive the access control lists for the objects from the capability list at the subjects. The existence of this means is advantageous since it allows the automatic derivation of access control lists which are required from a large number of security systems of installed computer systems. Therefore, the inventive system can be easily applied to existing computer systems without any modification of the security system of the installed computer systems. Furthermore, it is advantageous that this means derives the access control lists automatically and therefore a high data security and integrity within the computer system can be guaranteed. Furthermore, since the underlying access control mechanisms of existing security systems are used for access control checks at operation time, the inventive system does not lead to performance penalties and is scalable to the same degree as the underlying system.

In a further embodiment of the invention as described in claim 15 the inventive system comprises means for deriving the access control lists during a configuration step of the security system. This configuring step can be performed with or after each administration action. This means offers the advantage that the access control lists are actualized with each administration action and therefore guarantees high data security and integrity within the computer system. Furthermore, this means is advantageous since it guarantees the data security and integrity with less computing resources for the security system and requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment as described in claim 16 the inventive system comprises means for deriving the capability lists from a role-based access control system. The presence of this means allows the application of role-based access control systems as known from the prior art on security systems of computer systems as installed in the field in a large number. The inventive system allows advantageously the application of role-based access control systems without any modification or even new implementation on the installed security systems. Therefore, role-based access control systems can be provided for existing computer systems with low cost and high security and integrity of the data within the computer system.

In a further embodiment of the invention as described in claim 17 the inventive system comprises means for deriving and generating user accounts from the capability list. This is advantageous since it allows the automatic derivation and generation of user accounts on all computer systems that host objects occurring on the capability lists of subjects. This requires less efforts, thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

#### Brief Description of the Drawings

- Fig. 1 gives an overview of the method for controlling access rights.
- Fig. 2A gives an overview of role type instantiation.
- Fig. 2B shows an example for role type instantiation.
- Fig. 2C shows the example of role type instantiation of Fig. 2B in more detail.
- Fig. 3A shows the aspect of role type hierarchy of the inventive method.
- Fig. 3B shows an example of role type hierarchy for the business field of banking.
- Fig. 4 shows a method of resource set definition.
- Fig. 5 gives an overview of the method for controlling access rights on organizational level as on system level.
- Fig. 6 gives an overview of the system for authorization and control of access rights.
- Fig. 7 shows the possibility of a per-object-review as well as a per-subject-review as provided by the inventive system.

#### Description of a Preferred Embodiment

An elaborated preferred method for controlling access rights of subjects on objects in a computer system and a preferred embodiment of a system for authorizing and control of access rights according to the present invention will be described with reference to the accompanying drawings.

The Fig. 1 gives an overview of the method for controlling access rights. A set of subjects 1 as holders of access rights is defined and associated to a set of role types 2. The role types 2 are instantiated into a set of role instances 3 and therefore associates the subjects 1 to the role instances 3. Multiple subjects 1 can be associated with one role type 2. Also, a subject 1 can be associated with more than one role type 2. The instantiation of role types 2 into role instances 3 also determines the association between the role instances 3 and the objects 4 of the computer system. Usually there will be multiple instances of one role type due to different parameter values provided by different subjects.

The Fig. 2A gives an overview for the method of role type instantiation. Persons 5 that are users of an enterprise computer system are employees acting in assigned job positions 6. Each job position 6 is associated with a set of functional tasks and, thus, associates these tasks with a user in the enterprise organization hierarchy. Each task requires a set of competences, which can be viewed

as a set of specific access rights to a set of objects 4 necessary to carry out that task. Hence, each job position 6 ultimately associates a user with specific access rights to a set of objects 4. Thus, a security administrator must be able to associate these rights, objects, and transactions with the job positions of the enterprise organization. To enable this, the concepts of role types and role instances are defined.

The Fig. 2B shows job positions 6, role types 2, and the creation of role instances 3. The diagram shows an organization structure, e.g. organization units 7 and job positions 6, on the left and a set of role types 2 on the top of the matrix. An "X" in a field of the matrix means that a role instance 3 of the corresponding role type 2 is assigned to the job position 6. The necessary parameter values to instantiate the role type 2 are derived from attributes of the individual job position 6 or a higher level organization unit. The values of these attributes determine the actual competences the job position 6 is assigned via the role instance 3. Job positions 6 may share the same role instance 3 as illustrated by the shaded fields in a column.

A job position 6 is associated with one or more role instances 3, depending upon how granular the job position 6 is intended to be. These role instances 3 are derived from different role types 2. For example, there are three role instances associated with the job position "staff member 2" of "private loans", one derived from the role type "loan specialist", another one derived from "customer consultant", and one derived from "bank employee".

Often similar job positions, such as "staff member 1" and "staff member 2" of the "private loans" department, will be assigned to the same role instance as shown from the shaded fields in the matrix, because none of the attributes that are relevant for instantiating the role type differ between the job positions. However, different job positions 6 or similar job positions 6 in different organization units 7 will usually be associated with different role instances 3 of the same role type 2, because they bring in different attribute values for the role type instantiation. In the above example the role type "loan specialist" is instantiated in two different role instances that are bound to two different job positions of the department "object appraisal", the "team-leader" and the "staff member 1" position.

Job sharing can be modelled by assigning one job position 6 to multiple persons 5. On the other hand a single person 5 may be assigned to multiple job positions 6. For example, a person 5 in a "staff member" position in a department may also act, perhaps temporarily, as the "department manager". Of course, assignment to some job positions 6 may exclude assignment to other job positions 6 for separation-of-duty reasons. For example, a person 5 in the job position 6 "security administrator" may not be assigned to the job position 6 of "auditor" because otherwise the accountability of the "security administrator's" actions would be lost.

The Fig. 2C shows an example of the role type instantiation method in more detail, especially for the role instance in the framed matrix cell 15 of Fig. 2B. A role instance 3 binds the relative competences defined by a role type 2 to the objects 4, and access rights specific to an organization unit 7 or a job position 6. To perform this, at first for each organization unit and for each job position 6 a set of attributes has to be declared as relevant for role type instantiation. These attributes are said to be advertised. As an example, this could be the department identity or the location attribute of the department organization unit or the project identity attribute of a job position 6. Second, so-called relative resource sets 8 may be defined and associated with role types 2. A relative resource set 8 specifies the parameters it expects for instantiation from among the advertised ones in the enterprise. For example, one could define the relative resource set "printers" (printlocation) by enumerating the printers that are available to each location:

printers (Boeblingen): = {p2160, p2240, ...}  
 printers (Heidelberg): = {prt01, prt02, ...}

The "print location" parameter is declared as referencing the advertised "location" attribute of a department.

Thus, when a job position 6 as part of certain organization units 7 is combined with a role type 2 associated with parameterized relative resource sets 8, the actual resources can be determined by instantiating the parameters with the values of the advertised attributes for this job position 6. In the example of Fig. 2C, if

1. private loans is located in Heidelberg,
2. the relative resource set 8 "printers (printlocation)" is associated with role type 2 "bank employee" with permission "use", and
3. "staff member 1" of the department "private loans" is assigned the role type 2 "bank employee".

Then "staff member 1" will have "use" access to the printers "prt01, prt02, ...".

Whether a new role instance 3 has to be created in this case depends on whether the "bank employee" role type 2 has already been instantiated with the same parameters. If this is the case "staff member 1" will only be assigned the already existing role instance 3 "bank employee (... , Heidelberg, ...)".

Fig. 3A shows the role type hierarchy in the disclosed inventive method. The access-control policy semantics captured by the specification of role types reflect the functional partitioning and inclusion of generic access rights, resources, and transactions necessary to conduct the business activities and management of an enterprise. This partitioning and inclusion is intended to cover the data and application access relationships that are independent of the users job position 6 and organization context, i.e. units 7, of the enterprise. The rest of the access-control semantics captured by role instances 3 and job positions 6 reflect constraints placed by enterprise policies, such as the need-to-know and separation-of-duty policies, on enterprise organization units 7.

A role type 2 is defined as a set of generic parameter-dependent resources and their associated permissions or access rights. In a special case they may also contain concrete resources that do not depend on any parameters. Role types 2 can be organized hierarchically by a "subsumed" relation. If a first role type 16 subsumes a second role type 17 then the set of access rights available to an instance 18 of the first role type 16 includes those available to a corresponding instance 19 of the second role type 17. The expression "corresponding" in this context means that both role types 16, 17 are instantiated with the same parameter values. The subsuming role type 16 must have at least the parameters of the subsumed role type 17, it may have more.

The role type hierarchy defines in mathematical terms a lattice structure. Trivially, the top of the lattice can include all types of access rights to all objects 4, whereas the bottom can include the respective empty sets. Of course, lattices with non-trivial tops and bottoms can be defined. When instantiating a lattice of role types in a system, the top and bottom of the lattice need not be used for any specific role instance 3 and job position 6.

It is the implicit assumption which leads to the notion of the role type hierarchy that the sets of generic competences of job functions 6 and the role types 2 derived from them

1. can be structured as hierarchies by the subsumed relation, and
2. do not change very frequently.

The first assumption appears to be realistic because enterprise access control policies are often defined to reflect the hierarchical relationship built in an enterprise organization and functions. The second assumption also appears to be realistic because the job functions defined with an enterprise are stable since they are based on the enterprise business characteristics. Since the definition of job functions does not change very often, the sets of access rights to objects 4 needed for a job position 6 are not expected to change very often. It is important, that neither assumption prevents the addition of new role types 2 to the lattice nor that of new role instances 3 and job positions 6 to an enterprise.

The Fig. 3B shows an example for the role type hierarchy within the inventive method of access control. The example shows a hierarchy of the role types 2 used in Fig. 2B. In this example the access rights of a "second-line manager" and of a "first-line manager" subsume those of a "secretary" which in turn subsume those of a "typist". All role types subsume the role type "bank employee". As a consequence "bank employee" could be dropped from the matrix in Fig. 2B because the corresponding competences are covered by a membership in any of the other role types. For the same reason the "team-leader" of the "object appraisal" department does not have to be assigned the "loan specialist" role explicitly since his "team-leader" role type subsumes it.

The Fig. 4 shows the instantiation of concrete resource sets 9 and individual resources 10 from parameterized relative resource sets 8. The parameterized relative resource sets 8 are associated to the parameterized role types 2. The concrete resource sets 9 are derived from the parameterized relative resource sets 8 by using the parameter values provided from the subjects 6, 7 in the computer systems, e.g. provided from the job positions 6 and organization units 7 of the enterprise. The individual resources 10 are grouped to concrete resource sets 9. For example one possible parameterized relative resource set 8 is the resource set of "printers" with a parameter "printlocation". By providing the location parameter, for example location Heidelberg, the relative resource set 8 is instantiated into the concrete resource set 9 that includes all printers at the location Heidelberg. These printers at the location Heidelberg represent the individual resources 10.

The Fig. 5 shows an overview of the method for controlling access rights for the organizational level 20 as well as for the system level 21. It is shown that on the system level 21 persons 5 are represented as users 22, wherein one person 5 may have multiple user identifications, which may be derived from the role information and automatically generated (automatic registration) in the same way as the access rights are derived (automatic authorization). Furthermore, it is shown that the role instances 3 on the organization level 20 are represented by groups 23 on the system level. Furthermore, the concrete resource sets 9 are represented by the individual resources 10 on the system level 21.

The Fig. 6 shows a preferred embodiment of a system for authorization and control of access rights as disclosed in the present invention. It is shown that capability lists 30 associated to the subjects 1 of the computer system and containing the access rights of the respective subject 1 on the objects 4 of the computer system can be derived by appropriate means 32 into access control lists 31 associated to the objects 4 of the computer system and containing the access rights of the subjects 1 of the computer system on the respective object 4. The derivation means 32 can be implemented by hardware or by software. Furthermore, it is also possible to derive capability lists 30 from existing access control lists 31.

The Fig. 7 shows the possibility to perform a per-object review 40 with the inventive system for authorization and control of access rights. In this example the access rights may be an execute permission "X", a read permission "R" or a write permission "W". Since the inventive control system provides access control lists 31 associated with the objects 4 of the computer system it is possible to evaluate these access control lists 31 in order to determine all access rights of groups 23 within the computer system on the respective object 4. The group 23 is the representation of an instance, i.e. a role instance 3, of a parameterized role type 2. The role type 2 is instantiated by at least one parameter value provided by the job position 6. The person 5 assigned to this job position 6 has at least one user identification.



As also shown in Fig. 7, the inventive system for authorization and control of access rights as disclosed in the present invention offers the possibility to perform a per-subject review 41. The job position 6 to which a person 5 is assigned to is associated with a role. Associated to this role are the access rights of that role on the objects 4 of the computer system. The inventive system comprises capability lists 30 containing these access rights for each role. Furthermore, the system comprises deriving means 32 to generate new or modify existing access control lists 31 from the capability lists 30.

#### Claims

1. A method for controlling access rights of at least one subject (1) on at least one object (4) in a computer system, wherein said subject (1) is associated to at least one role, said method comprising the step of: controlling said access rights dependent on a membership of said subject (1) to said role, characterized in that a role type (2) is provided and said role is represented as a role instance (3) and said method further comprising the prior step of: instantiating said role type (2) into said role instance (3), that is, deriving said role instance (3) from said role type (2).
2. The method according to claim 1, wherein at least one parameter value is provided and said role type (2) is a parameterized role type (2), said method further comprising the step of: instantiating said parameterized role type (2) by using said parameter value.
3. The method according to claim 1 or 2, wherein at least one concrete resource set (9) is provided, said method further comprising the step of: providing said object (4) as an element of at least one of said concrete resource sets (9).
4. The method according to claim 3, wherein at least one parameter value is provided and at least one parameterized relative resource set (8) is provided, said method further comprising the step of: instantiating said parameterized relative resource set (8) into said concrete resource set (9) by using said parameter value, that is, deriving said concrete resource set (9) from said parameterized relative resource set (8) by using said parameter value.
5. The method according to one of claims 2 to 4, further comprising the step of: providing said parameter value by said subject (1).
6. The method according to claim 5, wherein a job position (6) within an organization unit (7) of the organization of said subject (1) is provided, said method further comprising the step of: providing said parameter value by said job position (6) or by said organization unit (7).
7. The method of claim 6, further comprising the step of: combining said job position (6) with at least one of said role types (2).
8. The method of one of claims 4 to 7, further comprising the step of: associating at least one of said parameterized relative resource sets (8) with said role types (2).
9. The method of one of claims 3 to 8, further comprising the step of: performing a configuring step for deriving said role instances (3) and for deriving said concrete resource sets (9) and objects (4).
10. The method of one of claims 3 to 9, further comprising the steps of: specifying capability list types associated with said role types (2), and performing a configuring step for deriving a capability list (30) associated with a corresponding role instance (3) from said capability list types, said capability list (30) provides said access rights of said role instance (3) on said objects (4).
11. The method of claim 9 or 10, further comprising the step of: generating or modifying access control lists (31) associated with said concrete resource sets (9) and objects (4), said access control lists (31) provide said access rights of said subjects (1) on said object (4).
12. The method of one of claims 1 to 11, wherein said role types (2) are organized hierarchically.
13. A computer system for registration, authorization, and control of access rights of at least one subject (1) on at least one object (4), said system comprises access control lists (31) at each object (4), said access control lists (31) provide said access rights of said subjects (1) on said object (4), characterized in that, said system further comprises: capability lists (30) associated with said subject (1), said capability lists (30) provide said access rights of said subject (1) on said objects (4).
14. The system according to claim 13, further comprising: means for deriving (32) said access control lists (31) at said objects (4) from said capability lists (30) associated with said subjects (1).



15. The system according to claim 13 or 14, further comprising:  
means for deriving (32) said access control lists (31) during a configuring step of said system.

5

16. The system according to one of claims 13 to 15, further comprising:  
means for deriving (32) said capability lists (30) from a role based access control system.

10

17. The system according to one of claims 13 to 16, further comprising means for deriving and generating necessary user accounts from said capability lists (30), in particular from the locations of objects (4) in said capability lists (30).

15

20

25

30

35

40

45

50

55

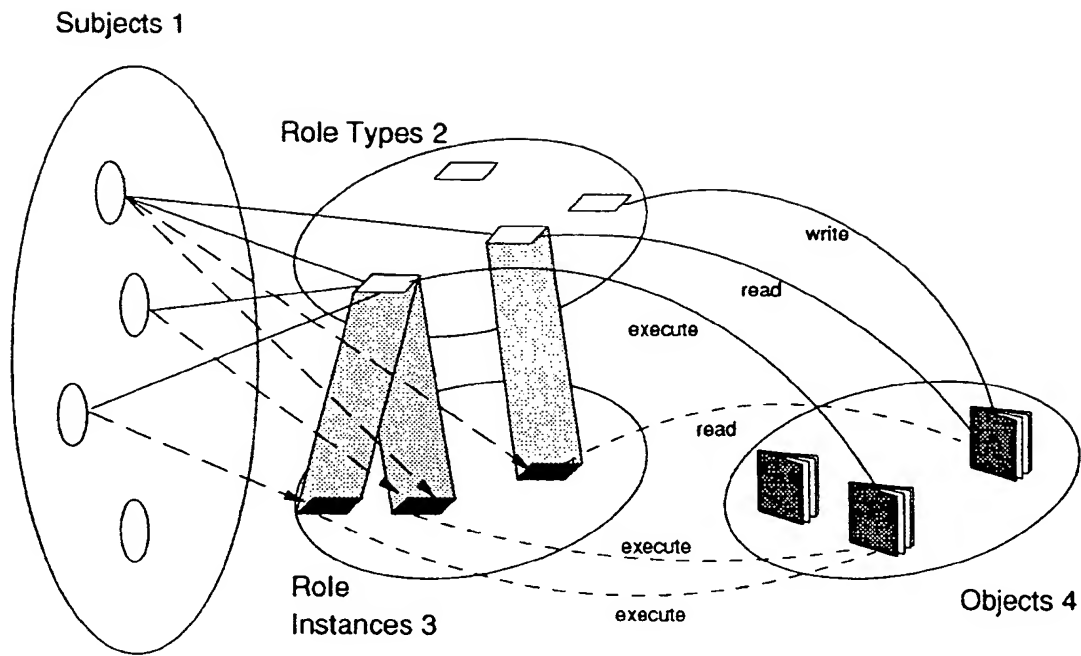


Fig. 1

BEST AVAILABLE COPY

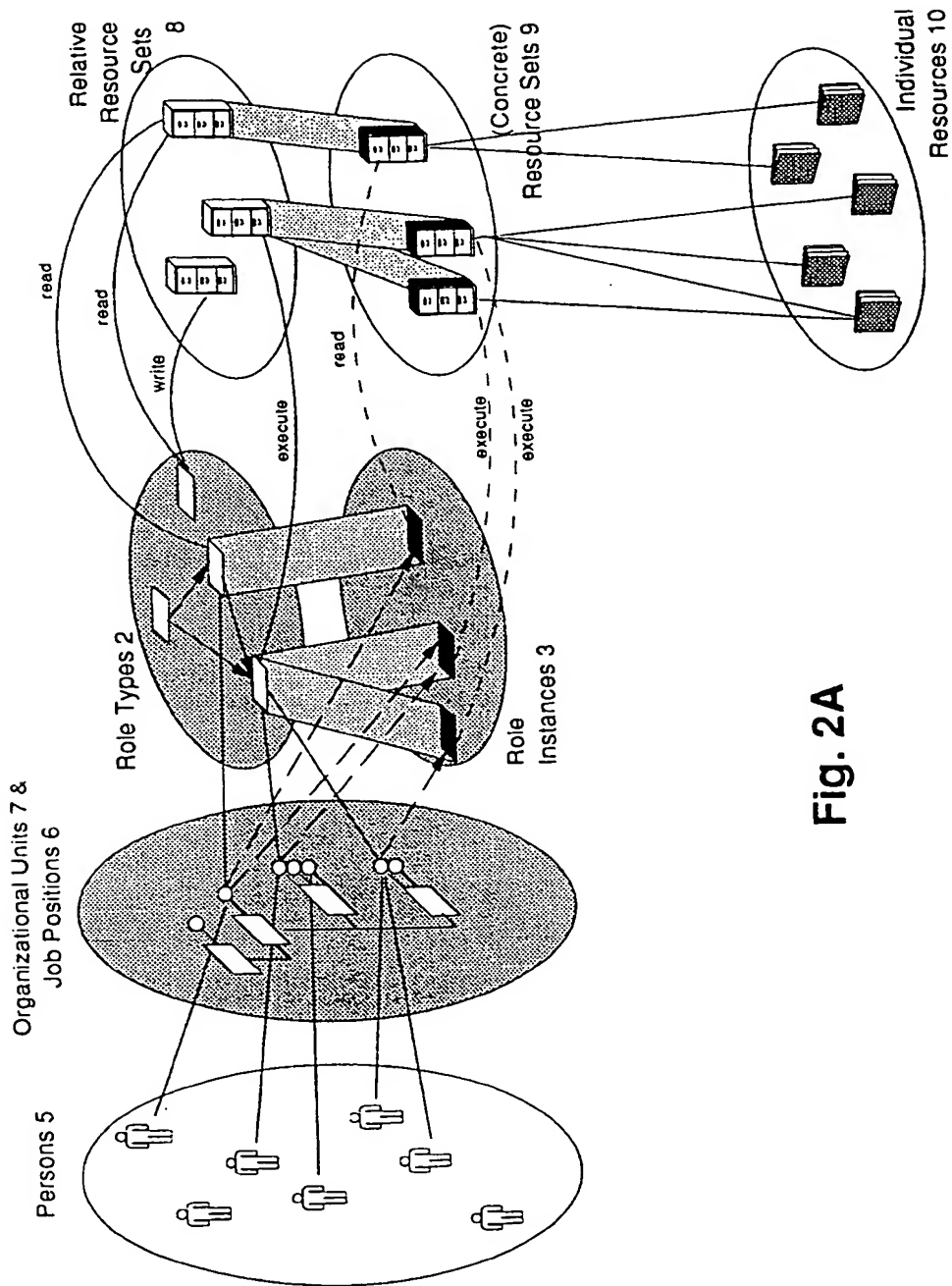


Fig. 2A

BEST AVAILABLE COPY

Org. Unit 7 Job Position 6		Role Type 2									
		2nd-Line Manager	1st-Line Manager	Team Leader (Role Type)	Loan Specialist	Customer Consultant	Typist	Object Appraiser	Archival Specialist	Secretary (Role Type)	Bank Employee
Real Estate Loans	Division Manager	x									x
										x	x
	Secretary									x	x
	Advisor			x				x			x
	Dept. Manager										x
	Team Leader			x	x						x
	Staff Member 1										x
	Staff Member 2										x
	Staff Member 3										x
	Advisor			x				x			x
Private Loans	Dept. Manager										x
	Team Leader			x	x						x
	Staff Member 1										x
	Staff Member 2										x
Object Appraisal	Dept. Manager										x
	Team Leader			x	x						x
	Staff Member 1										x
	Staff Member 2							x			x
Corporate Loans	Dept. Manager										x
	Team Leader										x
	Staff Member 1										x
	Staff Member 2										x
Secretary (Role Type)	Dept. Manager										x
	Team Leader										x
	Staff Member 1										x
	Staff Member 2										x
Bank Employee	Dept. Manager										x
	Team Leader										x
	Staff Member 1										x
	Staff Member 2										x

Fig. 2B

BEST AVAILABLE COPY

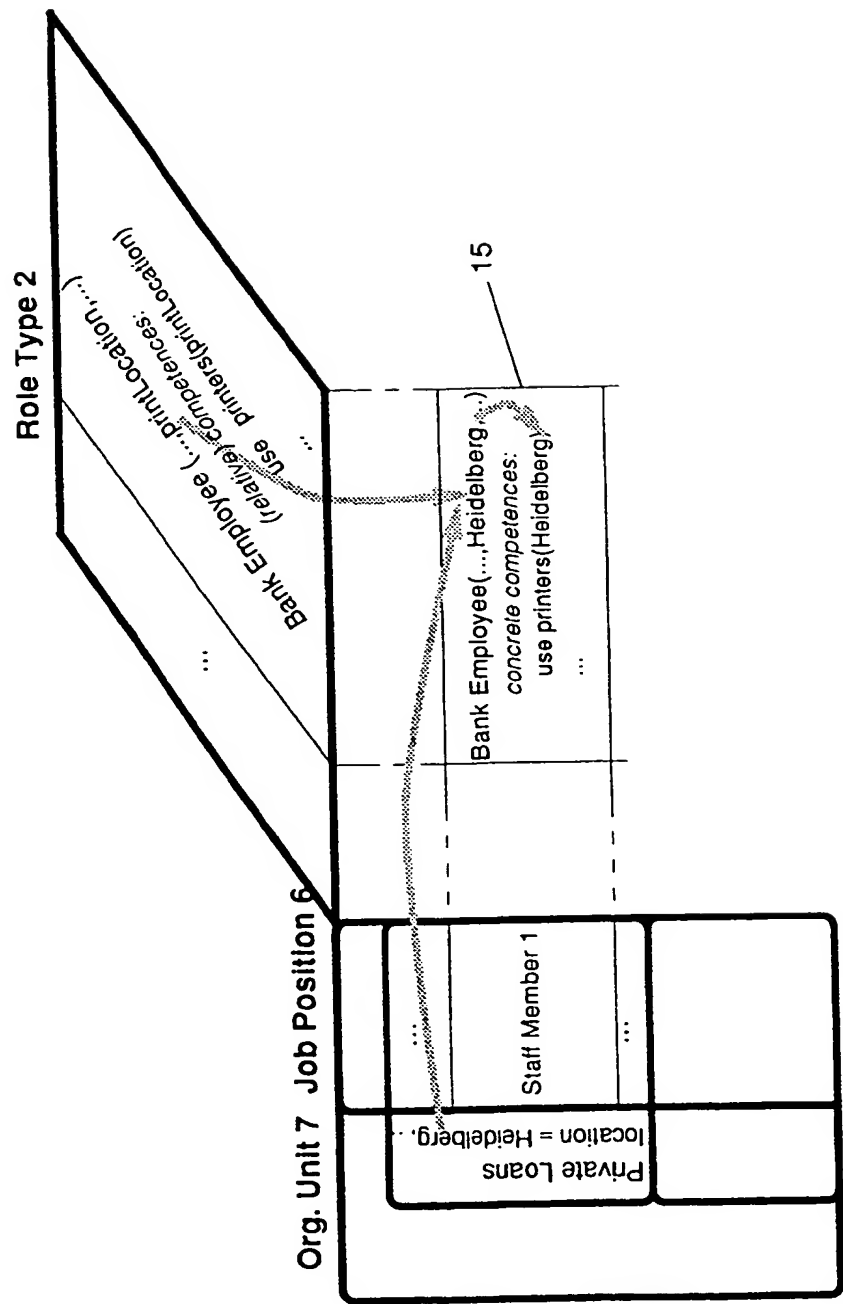


Fig. 2C

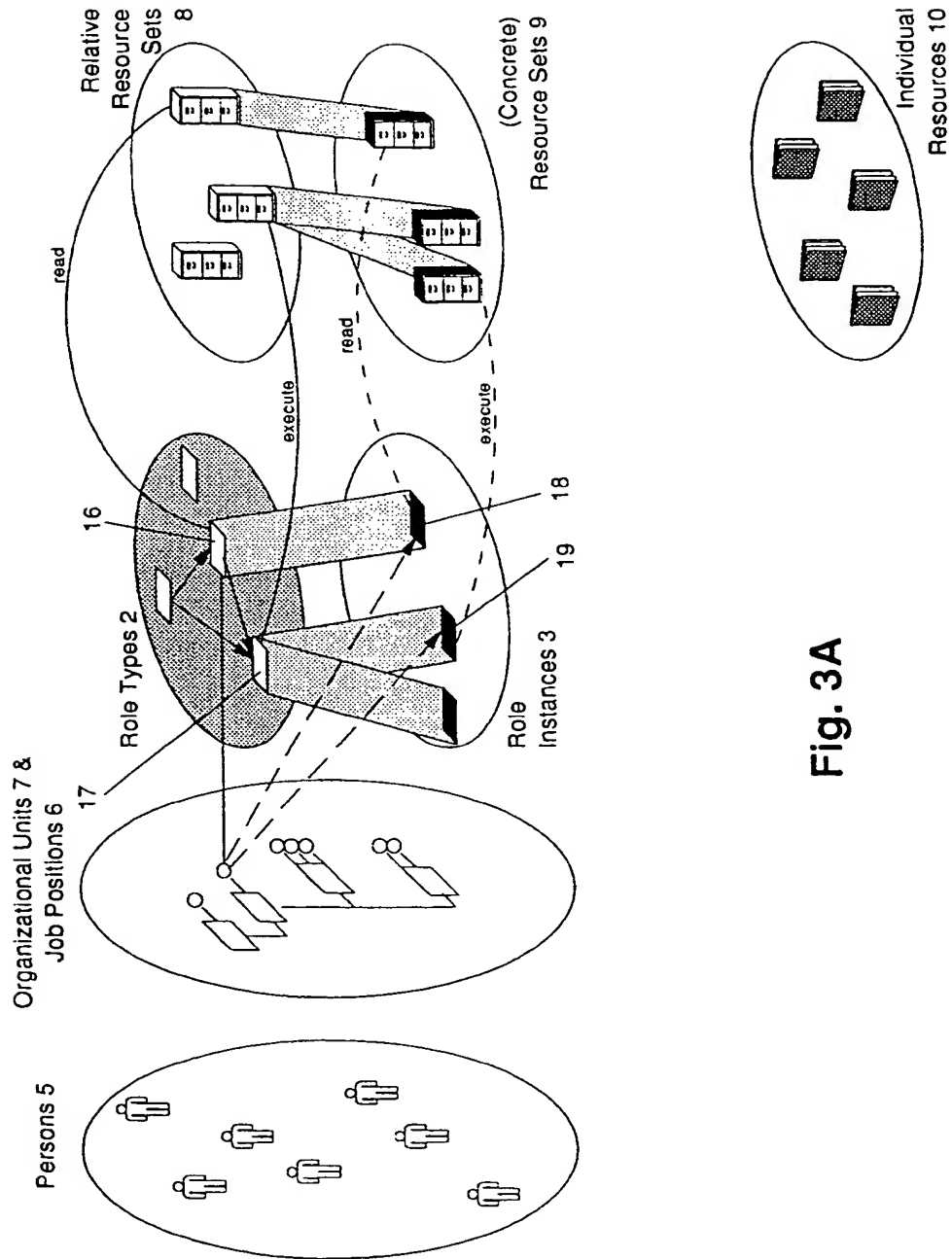


Fig. 3A

BEST AVAILABLE COPY

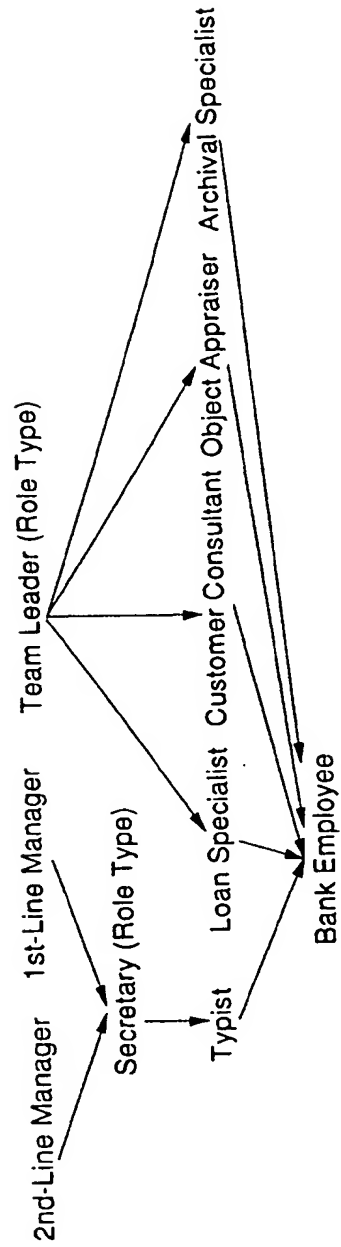


Fig. 3B



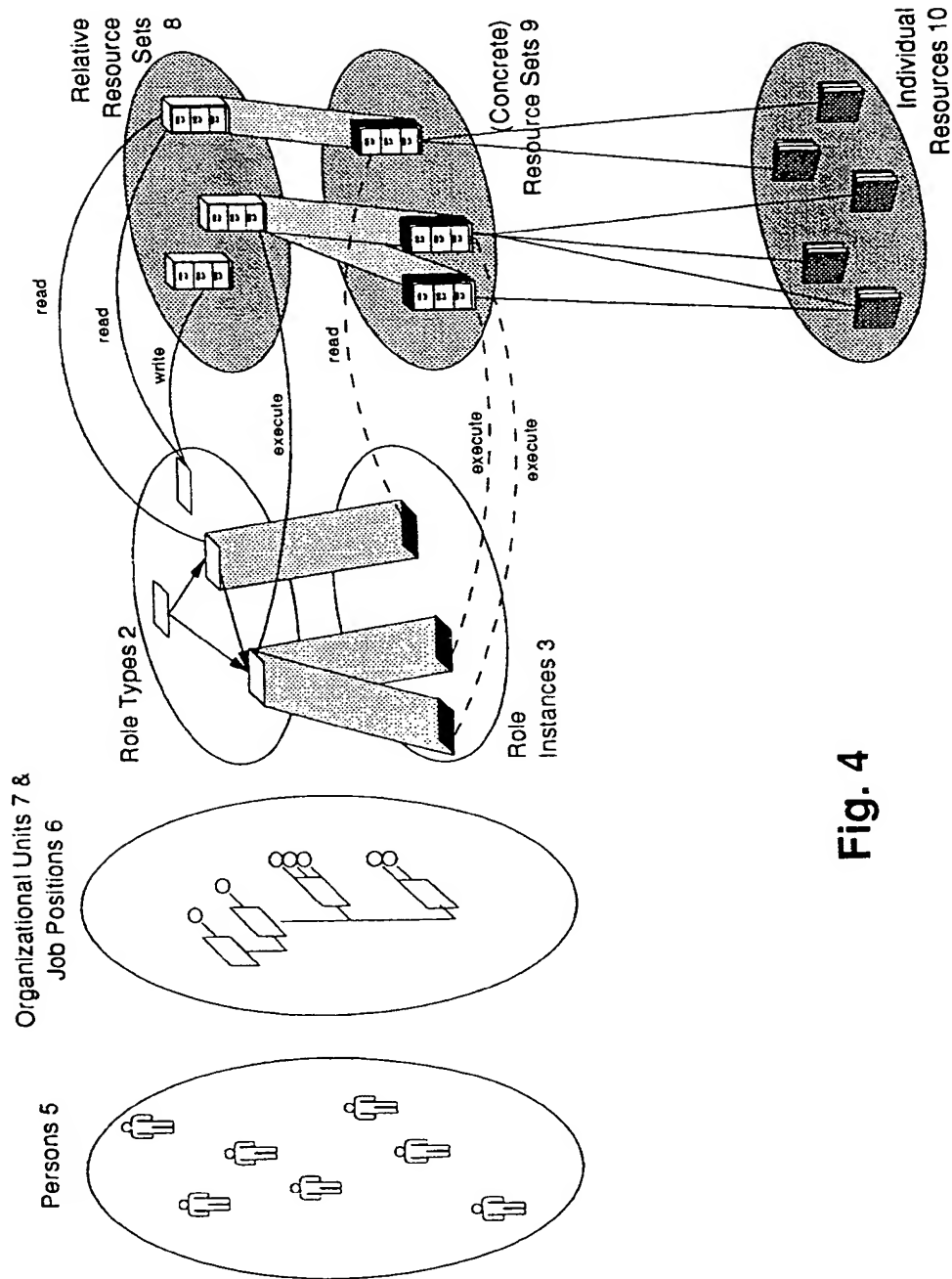
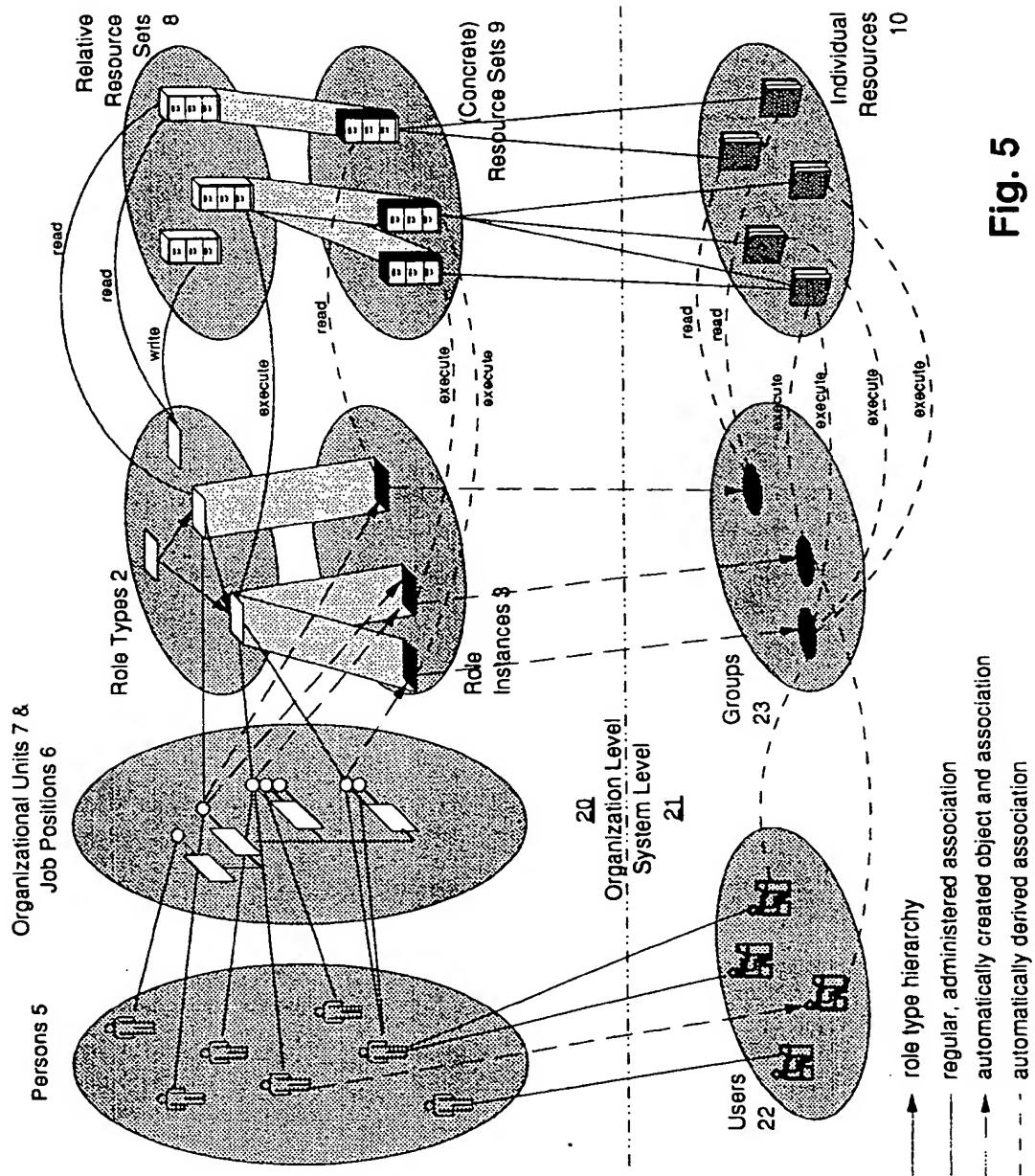


Fig. 4

BEST AVAILABLE COPY



**Fig. 5**

BEST AVAILABLE COPY

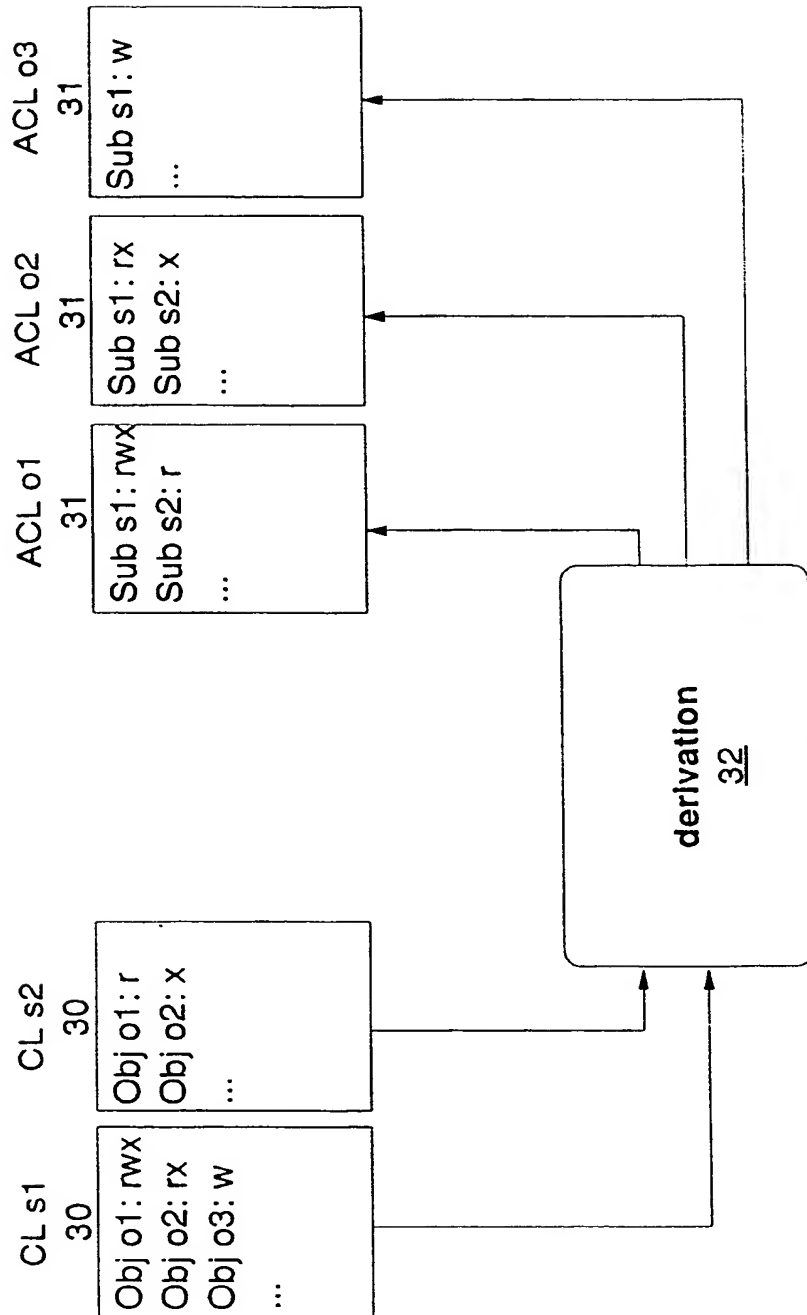


Fig. 6

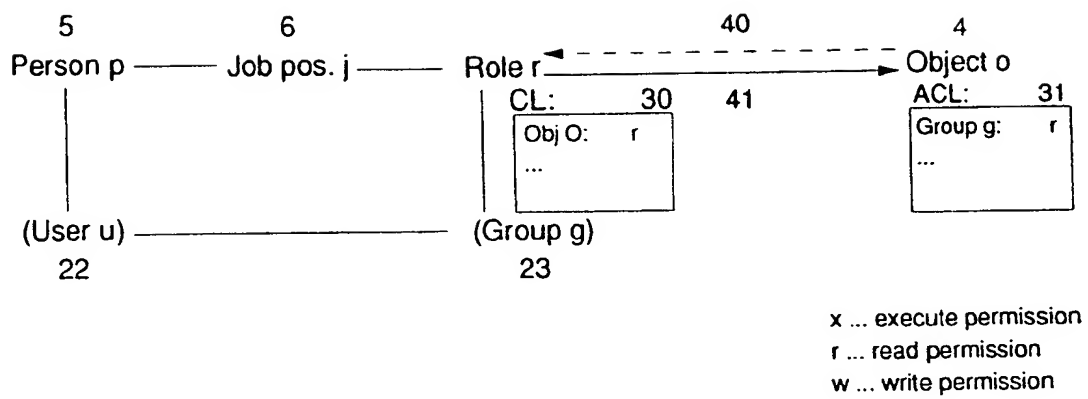


Fig. 7



European Patent  
Office

# EUROPEAN SEARCH REPORT

Application Number  
EP 94 11 2649

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
D,X	DATABASE SECURITY: STATUS AND PROSPECTS, 1988, NORTH-HOLLAND, NL; pages 209 - 222 F.H.LOCHOVSKY 'Role-Based Security in Database Management Systems' * page 211, line 3 - page 216, line 10 *	1,2,5-7, 12,13,15	G06F12/14 G06F1/00
D,Y	---	3,4, 9-11,14, 16,17	
Y	COMPUTER COMMUNICATIONS, vol.13, no.9, November 1990, GUILDFORD, GB; pages 571 - 580 J.MOFFETT ET AL 'Specifying Discretionary Access Control Policy for Distributed Systems' * page 572, left column, line 19 - page 574, right column, line 9 *	3,4,9,11	
D,Y	IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, 9 May 1990, OAKLAND, US; pages 116 - 132 R.W.BALDWIN 'Naming and Grouping Privileges to Simplify Security Management in Large Databases' * page 116, right column, paragraph 1 * * page 117, right column, paragraph 4 - page 118, left column, paragraph 2 * * page 119, left column, paragraph 2 - right column, paragraph 2 * * page 128, left column, paragraph 4 - right column, paragraph 3 * * page 131, left column, paragraph 4 - right column, paragraph 3 * --- -/--	9,11,14, 17	TECHNICAL FIELDS SEARCHED (Int.Cl.6)  G06F
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		14 November 1994	Powell, D
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03/82 (P04C01)



European Patent  
Office

# EUROPEAN SEARCH REPORT

Application Number  
EP 94 11 2649

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
Y	IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY, 21 February 1988, OAKLAND, US; pages 39 - 49 S.T.VINTER 'Extended Discretionary Access Controls' * page 47, left column, paragraph 3 -paragraph 4 *	10, 16	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 14 November 1994	Examiner Powell, D
<p><b>CATEGORY OF CITED DOCUMENTS</b></p> <p>X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document</p> <p>T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application I : document cited for other reasons &amp; : member of the same patent family, corresponding document</p>			

EPO FORM 1503 03.82 (POMC01)

**THIS PAGE BLANK (USPTO)**